UNITED STATES DISTRICT COURT

for the

Eastern District of North Carolina

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Jonathan Albert Carter, b/m, 5'10", DOB 10/14/1980, FL
DL # C636-421-80-374-0

Case No. 7:24-mj-1014-RJ

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

Jonathan Albert Carter, as further described in Attachment A

located in the Eastern District of North Carolina, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B hereto and incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2252A	Distribution, Receipt, and/or Possession Child Pornography

The application is based on these facts:
See attached affidavit which is attached hereto and incorporated herein by reference

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

KERRIE HARNEY Digitally signed by KERRIE HARNEY Date: 2024.01.24 08:51:18 -05'00'

Applicant's signature

Kerrie L. Harney, S/A Federal Bureau of Investigation

Printed name and title

On this day, Kerrie Harney ~~January 24 2024~~ appeared before me via reliable electronic means, was placed under oath, and attested to the contents of this Application for a Search Warrant.

Date: January 24 2024

Judge's signature

City and state: Wilmington, North Carolina

Robert B. Jones, Jr., United States Magistrate Judge

Printed name and title

STATE OF FLORIDA **CASE NO.** 7:24-mj-1014-RJ

COUNTY OF ORANGE

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Kerrie L. Harney, being duly sworn, do hereby depose and state as follows:

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI) and have been since June 2016. I currently serve as an investigator for the FBI Crimes Against Children/Innocent Images Unit in Orlando, Florida. As an investigator for the FBI Crimes Against Children Task Force, my responsibilities include investigating possible criminal violations of Title 18 of the United States Code.

2. I have received specialized training in the investigations of sex crimes, child exploitation, child pornography, and computer crimes. I have been involved in investigations involving child pornography and online solicitation/enticement of a minor. I have participated in investigations of persons suspected of violating federal child-exploitation laws, including 18 U.S.C. §§ 2242, 2251(a) and (e), 2252, and 2252A. I have also participated in various training courses for the investigation and enforcement of federal child pornography laws in which computers and cellular phones are used as the means for receiving, transmitting, and storing child pornography. Additionally, I have participated in the execution of search warrants involving searches and seizures of computers, computer equipment, software, and electronically stored information.

3. I submit this affidavit in support of an application under Federal Rule of Criminal Procedure 41 for a warrant to search the person of Jonathan Carter ("TARGET PERSON"), as more fully described in Attachment A. As detailed below, probable cause exists that evidence, fruit, contraband and/or instrumentalities of violations of 18 U.S.C. §§ 2252A(a)(2) (receipt and distribution of child pornography) and 2252A(a)(5)(B) (possession of child pornography) are located on the TARGET PERSON, as more specifically detailed in Attachment B.

4. I make this affidavit from personal knowledge based on my participation in this investigation, information from other criminal investigators, information from law-enforcement officers, information from agency reports, and the review of documents provided to me by these witnesses and law-enforcement officers.

5. This affidavit is being submitted for the limited purpose of seeking a search warrant, and I therefore have not set forth every fact learned during this investigation.

PROBABLE CAUSE

6. On January 26, 2023, the New York State Police received Cybertip #149466793 from the National Center for Missing and Exploited Children (NCMEC). NCMEC received the Cybertip from Yahoo! Inc. and detailed the transmission of 20 images of alleged Child Sexual Abuse Material (CSAM) from Yahoo account "jettolip@yahoo.com" sent via email. The images were sent on January 4, 2023, between the hours of 15:35:47 UTC-5 and 18:37:39 UTC-5. The

Cybertip provided the name "Jonathan Carter", phone number 404-444-6680, date of birth: 10/14/1980, email address: "jettolip@yahoo.com" and ESP User ID: X2RLZV45B6LZHPKUJWQDAY4TJY. Recovery email addresses were listed as "jettolip04@hotmail.com" and Jonathan.albert.carter@gmail.com. Multiple IP addresses were provided in the Cybertip, which were used to access the Yahoo account in Secaucus, NJ (Clouvider Limited), Homestead, FL (Comcast Business), Rochester, NY, Miami, FL, and Queens, NY (AT&T Wireless). The PDF file and images of alleged CSAM were reviewed by New York State Police and the Department of Homeland Security Investigations (HSI) and were determined to be Child Sexual Abuse Material (CSAM). Pursuant to a subpoena issued by HSI, the subscriber information for 404-444-6680 was identified as:

Name: Jonathan Carter

Address: 7051 Narcoossee Road Orlando, FL 32822

7. On February 15, 2023, Cybertip #149466793 was transferred to the Orlando Police Department. The 20 files of alleged CSAM were viewed by the Electronic Service Provider (ESP) and contained the lewd exhibition of female pre-pubescent vaginas and anuses; the rape of pre-pubescent female children by adult males; pre-pubescent females forced to perform fellatio on an adult male; adult male attempting to rape an infant female child and digitally penetrate the infant's vagina.

8. A search of investigative resources revealed a Florida Driver license in the name of Jonathan Carter with the same date of birth listed in the Cybertip as

10/14/1980. His driver's license showed an address of 6441 S. Chickasaw Trail in Orlando, Florida. The address of 7051 Narcoossee Road from the AT&T subpoena belongs to an AT&T store and the address of 6441 S. Chickasaw Trail from Carter's driver's license belongs to a UPS store. A review of investigative resources revealed that Jonathan Carter is a licensed airline transport pilot, licensed since February 22, 2022. It is unknown where Carter currently resides.

9. On March 12, 2023, a search warrant was obtained and issued to Yahoo for email address jettolip@yahoo.com, and a response was provided by Yahoo on March 18, 2023. A review of the email account showed the email account belongs to Jonathan Carter and showed multiple travel arrangements from Spirit and United Airlines flight confirmations and cancellations. The email also contained a number of emails attributable to Carter including Amazon orders in the name of Carter delivered to an Amazon locker in Orlando, FL, a rental car reservation in the name of Carter that shows Carter as "United Airlines personnel", and several hotel reservation confirmations in the name of Carter.

10. On March 18, 2023, investigative subpoenas were issued for multiple AT&T IP addresses and one Comcast Business IP address, which logged into the Yahoo! Inc account. On April 14, 2023, AT&T provided a response to the investigative subpoena "Individual IP assignments within this block are not stored by AT&T. AT&T does not have individual IP records for the IPs in question". On May 9, 2023, a response was received from Comcast and the subscriber was identified as:

Name: Hawthorn Suites West Palm Beach

Address: 301 Lamberton Drive West Palm Beach, FL 33401

11. Employment records for Carter revealed he is employed by GoJet Airlines and listed his name as Jonathan Carter with the same date of birth 10/14/1980 and phone number 404-444-6680 from the CyberTip. The address listed showed the UPS store located at 10401 Post Office Blvd W #1522 in Orlando, Florida.

12. In May 2023, a state search warrant was issued to AT&T for cell tower location data for phone number 404-444-6680. Information from this return indicated that on January 4, 2023, between the hours of 15:35:47 UTC-5 and 18:37:39 UTC-5 the device utilizing that phone number was in Daytona Beach, FL.

13. Carter is an airline pilot who is scheduled to pilot flight number UA 4422 from Newark, New Jersey to Wilmington, North Carolina on January 25, 2024 arriving in Wilmington at 3:18 p.m. Per Carter's employer, he is required to fly with his cellular telephone and tablet.

RELEVANT INFORMATION REGARDING PERSONS INVOLVED IN THE POSSESSION AND DISTRIBUTION OF CHILD PORNOGRAPHY

14. Based upon my knowledge and experience in child sexual exploitation and child pornography investigations, I know the following:

a. Persons who are involved with child pornography generally have other sexually explicit materials related to their interest in children, which may

consist of photographs, motion pictures, videos, text material, computer graphics and digital or other images for their own sexual gratification, often including child erotica, which may consist of images or text writing involving sex with minors that do not rise to the level of child pornography but nonetheless fuel their deviant sexual fantasies involving minors. I am aware that this sort of material has been admitted in trials under Fed. R. Evid. 404(b) to prove such things as the possessor's knowledge, intent, motive, and identity and under Fed. R. Evid. 414 to prove the person has a sexual interest in minors.

b. Individuals who collect child pornography often seek out like-minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica. They do this to gain status, trust, acceptance, and support and to increase their collection of illicit images and child erotica. The different Internet-based vehicles used by such individuals to communicate with each other include, but are not limited to, P2P chat and file sharing programs, e-mail, e-mail groups, bulletin boards, Internet Relay Chat (IRC), newsgroups, Internet clubs, and various forms of Instant Messaging such as Yahoo Messaging, and "chat" that is sometimes saved on the user's computer or other digital storage media.

c. Besides sexual photos of minors and child erotica, such individuals often produce and/or collect other written material on the subject of sexual activities with minors, which range from fantasy stories to medical,

sociological, and psychological writings, which they save to understand and justify their illicit behavior and desires.

d. Individuals who collect child pornography often collect, read, copy, or maintain names, addresses, including e-mail addresses, phone numbers, and lists of persons who have advertised or otherwise made known in publications and on the Internet that they have similar sexual interests, or have child pornography and child erotica for sale or trade. These contacts are maintained for personal referral, exchange or, sometimes, commercial profit. They may maintain these names on computer storage devices, web sites or other Internet addresses, and their discovery can serve as leads to assist law enforcement in proving the instant case and in apprehending others involved in the underground trafficking of child pornography.

e. Individuals who collect child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect from discovery, theft, and damage their collections of illicit materials. The known desire of such individuals to retain child pornography, together with the sense of security afforded by using computers, provides probable cause to believe that computer images, especially child pornography and erotic nudity involving minors, will be retained by the collector indefinitely. These individuals may protect their illicit materials by passwords, encryption, and other security measures, save it on movable media such as CDs, DVDs, flash memory, thumb drives, and removable hard drives, which can be very small in size, including as small as a postage stamp, and easily secreted, or send it to third party image storage sites via the Internet.

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

15. Computers and computer technology have revolutionized the way in which individuals interested in child pornography interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. There were definable costs involved with the production of pornographic images. To distribute these on any scale required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contacts, mailings, and telephone calls. The development of computers has changed this. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

16. Child pornographers can now transfer photographs from a camera onto a computer-readable format with a device known as a scanner. With the advent of digital cameras, the images can now be transferred directly onto a computer. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world.

17. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers and

mobile phones has grown tremendously within the last several years. These drives can store thousands of images at very high resolution.

18. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

19. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet portals such as Snapchat, Kik, and Dropbox, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services, as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

20. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or Internet service provider client software, among others). In addition to electronic communications, a computer user's Internet activities generally

leave traces or "footprints" and history files of the browser used. A forensic examiner often can recover evidence suggesting whether a computer contains wireless software, was running certain programs, and when certain files under investigation were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

21. Internet computers identify each other by an Internet Protocol or IP address. When a computer connects to the Internet, the Internet Service Provider (ISP) providing the Internet connection assigns that computer a specific numerical identifier called an IP address. The IP address allows the computer to communicate with the Internet. ISPs control blocks of IP addresses and only assign a given IP address to one customer at a time. IP addresses are analogous to telephone numbers. To use a telephone, the phone must have an associated phone number. To access the Internet, a computer must be assigned an IP Address. IP addresses can be dynamic or static. Dynamic IP addresses can and do change over time; however, dynamic IP addresses can be retained by a subscriber for months or even a year or more, especially in cases where there is a high-speed cable modem connection, like the connection in this case Static IP addresses never change unless the customer cancels the account or requests a new static IP address.

22. I know that these IP addresses can assist law enforcement in finding a particular computer on the Internet. Once an IP address is known, a subpoena can be issued to the appropriate ISP for business records related to the subscriber assigned to that IP address at a particular time and date. The ISP typically provides information

concerning the name, address, and other identifying information of the subscriber using the particular ISP. This process has proven to be very reliable in identifying suspects using the Internet.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

23. As described in the foregoing paragraphs and in Attachments A and B, this application seeks permission to search and seize records that might be found on the TARGET PERSON, in whatever form they are found. One form in which the records might be found is stored on a computer's hard drive or other storage media. Some of these electronic records might take the form of files, documents, and other data that is user-generated. Some of these electronic records, as explained below, might take a form that becomes meaningful only upon forensic analysis. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

24. *Probable cause.* I submit that if a computer or storage medium is found on the TARGET PERSON, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at

little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

25. *Forensic evidence*. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence

of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium on the TARGET PERSON because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or

absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating, or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the

computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

d. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

e. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

f. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

g. I know that when an individual uses a computer to possess child pornography and to distribute child pornography over the Internet, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

26. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search for information that might be stored on storage media often requires the seizure of the physical storage media and later, off-site review consistent with the warrant. In lieu seizing devices or media for off-site review, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. *The time required for an examination.* As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. *Technical requirements.* Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

27. *Nature of examination*. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

UNLOCKING MOBILE DEVICES USING BIOMETRIC DATA

28. It is likely that personal electronic devices found on the TARGET PERSON will contain security software that is unlockable using biometric data, and I request that this Court authorize law enforcement officers to press the fingers (including thumbs) of the TARGET PERSON to the mobile devices' fingerprint sensors (if the sensor exists) or present the TARGET PERSON's irises or face to the device(s)' cameras during the search, in an attempt to unlock the device(s) for the purpose of executing the search authorized by these warrants.[1]

[1] Based on my training and experience, I know that a person's "identifying physical characteristic[s]" are not testimonial and thus fall "outside [the] protection" of the Fifth Amendment. *Gilbert v. California*, 388 U.S. 263, 267 (1967). The privilege against self-incrimination is not violated by an order compelling a person to submit to photographing and measurements or to provide fingerprints, writing samples, or voice exemplars. *See, e.g., United States v. Dionisio*, 410 U.S. 1, 7 (1973); *California v. Byers*, 402 U.S. 424, 431-32 (1971); *Gilbert*, 388 U.S. at 266-67; *Schmerber v. California*, 384 U.S. 757, 763-64 & n.8 (1966); *see also In the Matter of the Search of [Redacted] Washington, District of Columbia*, 2018 WL 3155596 (D.D.C. 2018) (search warrant authorizing compelled use of biometric feature to unlock devices did not violate Fourth or Fifth Amendments).

29. The warrant I am applying for would permit law enforcement to obtain from the TARGET PERSON the display of physical biometric characteristics (such as fingerprint, thumbprint, or facial characteristics) in order to unlock devices subject to search and seizure pursuant to this warrant. I seek this authority based on the following:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices, and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners and facial recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, Apple offers a facial recognition feature called "Face ID." During the Face ID registration process, the user holds the device in front of his or her face. The device's camera then analyzes, and records data based on the user's facial characteristics. The device can then be unlocked if the camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Face ID.

d. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

e. As discussed in this affidavit, based on my training, and experience I believe that one or more digital devices will be found during the search. The passcode or password that would unlock the device(s) subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device(s), making the

use of biometric features necessary to the execution of the search authorized by this warrant.

f. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 4 hours *and* the passcode or password has not been entered in the last 156 hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

g. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose physical characteristics are among those that will unlock the device via biometric features, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the

device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any individual, who is found at the Subject Premises and reasonably believed by law enforcement to be a user of the device, to unlock the device using biometric features in the same manner as discussed above.

h. Due to the foregoing, if law enforcement personnel encounter a device that is subject to search and seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to (1) press or swipe the fingers (including thumbs) of any individual, who is found at the subject premises and reasonably believed by law enforcement to be a user of the device, to the fingerprint scanner of the device; (2) hold the device in front of the face of those same individuals and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search its contents as authorized by this warrant.

DEFINITIONS

30. The following definitions apply to this affidavit and to Attachment B:

a. "Child Erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

b. "Child Pornography," as used herein, includes the definition in 18 U.S.C. § 2256(8), which defines child pornography as any visual depiction of

sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. *See* 18 U.S.C. § 2256(2).

c. "Visual depictions," include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. *See* 18 U.S.C. § 2256(5).

d. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. *See* 18 U.S.C. § 2256(2).

e. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include:

storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

f. "Computer," as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1) as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

g. "Computer hardware," as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, flash memory cards, thumb drives and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts

that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

h. "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

i. "Computer-related documentation," as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

j. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

k. The terms "records," "documents," and "materials," used herein include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as digital cameras, floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, laptop computers or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical, or electronic storage device.

l. Kik Messenger (commonly known as Kik) is a freeware instant messaging mobile application that can be used to transmit and receive messages, photos, videos, sketches, mobile webpages, and other content. KIK users can communicate privately with other users or in groups.

m. Kik uses a smartphone's Internet connectivity to transmit and receive messages, photos, videos, and other content. KIK is known for protecting its users' anonymity by not requiring users to provide a telephone number during the Kik user registration process. The Kik application does log each user's IP addresses,

however, and those IP addresses can be used to determine the location in which Kik was used at particular points in time.

CONCLUSION

31. Probable cause exists that the TARGET PERSON, detailed in Attachment A, possesses on his person evidence, instrumentalities, contraband, and/or fruits of violations of 18 U.S.C. §§ 2252A(a)(2) (receipt and distribution of child pornography) and 2252A(a)(5)(B) (possession of child pornography) . I therefore seek permission to search the TARGET PERSON and to seize the items detailed in Attachment B.

Kerrie L. Harney, Special Agent
Federal Bureau of Investigation

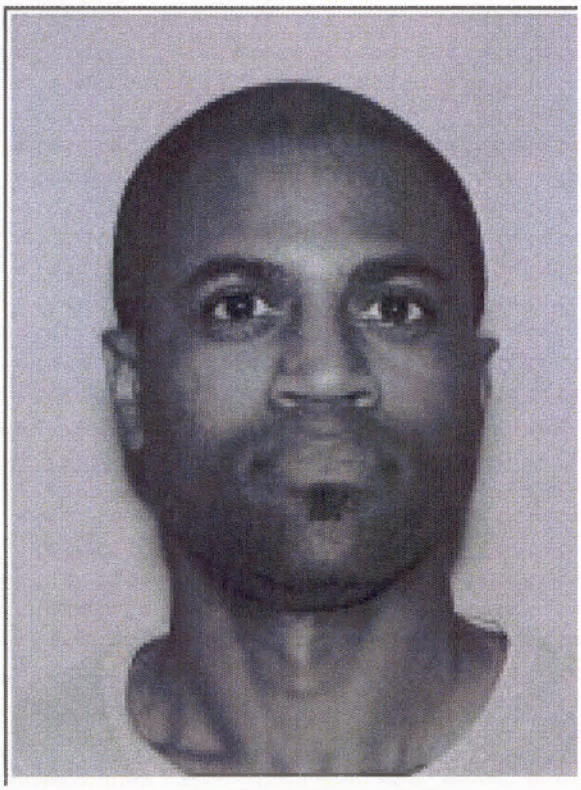
Sworn to via telephone after submission by reliable electronic means, pursuant to Fed. R. Crim. P. 4.1 and 41(d)(3), this 24 day of January 2024.

ROBERT B. JONES, JR.
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

PERSON TO BE SEARCHED

The TARGET PERSON, JONATHAN ALBERT CARTER, is a black male. Government records indicate that he is 5 feet, 10 inches tall. His birthdate is 10/14/1980. His Florida Driver's License Number is C636-421-80-374-0. A photograph of CARTER is below:



ATTACHMENT B

Property to be searched and seized

The following items to be searched and seized constitute instrumentalities, contraband, fruits, and/or evidence of violations of 18 U.S.C. §§ 2252A(a)(2) (receipt and distribution of child pornography) and 2252A(a)(5)(B) (possession of child pornography), which may be found in the possession of the TARGET PERSON detailed in Attachment A, including:

a. Any mobile device, cell phone device, or computer in the possession of the TARGET PERSON.

b. Any travel bags in the possession of the TARGET PERSON.

c. Images of child pornography, as defined in 18 U.S.C. § 2256.

c. Any record or document pertaining to the possession, receipt, and/or distribution of child pornography, as defined in 18 U.S.C. § 2256.

d. Any record or document identifying persons transmitting, through interstate commerce, including by computer, any visual depiction of a minor engaged in sexually explicit conduct, as defined in 18 U.S.C.§ 2256.

e. Any record or document bearing on the production, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate commerce, including by computer, of any visual depiction of a minor engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256.

f. Any record or document pertaining to the *preparation, purchase, and acquisition of names or lists of names* to be used in connection with the purchase, sale, trade, or transmission, through interstate commerce, of any visual depiction of a minor engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256.

g. Any record or document which lists names and addresses of any minor visually depicted while engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256.

h. Any record or document which shows the offer to transmit through interstate commerce any depictions of a minor engaged in sexually explicit conduct, as defined in 18 U.S.C.§ 2256.

i. Any record or documents which shows the transfer of obscene materials or images to a minor.

j. Any and all materials or items which are sexually arousing to individuals who are interested in minors, but which are not in and of themselves obscene or which do not necessarily depict minors involved in sexually explicit conduct. Such material is commonly known as "child erotica" and includes written materials dealing with child development, sex education, child pornography, sexual abuse of children, incest, child prostitution, missing children, investigative techniques of child exploitation, sexual disorders, pedophilia, nudist publications, diaries, and fantasy writings. "Child erotica" may also include, in this context, sex aids and/or toys.

k. Electronically stored communications or messages reflecting computer on-line chat sessions or e-mail messages with, or about, a minor that are sexually explicit in nature, as defined in 18 U.S.C. § 2256.

l. Storage media used as a means to commit the violations described above.

m. For any computer, to include, cell phones, or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

1. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

2. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

3. evidence of the lack of such malicious software;

4. evidence indicating how and when the COMPUTER was accessed or used to determine the chronological context of COMPUTER

access, use, and events relating to crime under investigation and to the COMPUTER user;

5. evidence indicating the COMPUTER user's state of mind as it relates to the crime under investigation;

6. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

7. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

8. evidence of the times the COMPUTER was used;

9. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

10. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

11. records of or information about Internet Protocol addresses used by the COMPUTER;

12. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

13. contextual information necessary to understand the evidence described in this attachment.

14. Any and all evidence referenced above in Attachment B, subsections a. through l.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "COMPUTER" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

This warrant also authorizes law enforcement, during the execution of the search warrant, to utilize the identifying-physical characteristics of the TARGET PERSON in order to open any COMPUTER, identify the COMPUTER(S)' user(s), determine which COMPUTER(S) to seize, and to search the COMPUTER(S) as authorized by this warrant.